L Number	Hits	Search Text	DB	Time stamp
6	76	(((database$1 OR register$1 OR registr$3 OR administrator$1 OR agent$1 OR vendor$ OR server$1 OR station$1) SAME ((person$4 OR user$2 OR subscriber$2 OR customer$2 OR individual$2 OR party$1) NEAR4 (information OR data OR attribute$1 OR detail$1 OR characteristic$1)) SAME (((secur$4 OR access$4 OR authoriz$6 OR authoris$6) NEAR4 (level$1 OR categor$3 OR option$1)) OR privilege$1))) AND ((person$4 OR user$2 OR subscriber$2 OR customer$2 OR individual$2 OR party$1) NEAR4 (information OR data OR attribute$1 OR detail$1 OR characteristic$1)) WITH (transmi$6 OR send$4 OR forward$4 OR transfer$6 OR receiv$4 OR download$4 OR retriev$4)	EPO; JPO; DERWENT	2002/12/30 05:00
7	47	((((database$1 OR register$1 OR registr$3 OR administrator$1 OR agent$1 OR vendor$ OR server$1 OR station$1) SAME ((person$4 OR user$2 OR subscriber$2 OR customer$2 OR individual$2 OR party$1) NEAR4 (information OR data OR attribute$1 OR detail$1 OR characteristic$1)) SAME (((secur$4 OR access$4 OR authoriz$6 OR authoris$6) NEAR4 (level$1 OR categor$3 OR option$1)) OR privilege$1))) AND ((person$4 OR user$2 OR subscriber$2 OR customer$2 OR individual$2 OR party$1) NEAR4 (information OR data OR attribute$1 OR detail$1 OR characteristic$1)) WITH (transmi$6 OR send$4 OR forward$4 OR transfer$6 OR receiv$4 OR download$4 OR retriev$4)) AND (((secur$4 OR access$4 OR authoriz$6 OR authoris$6 OR privilege$1) NEAR4 (level$1 OR categor$3 OR option$1 OR zon$3 OR layer$3 OR grain$1 OR granular$4 OR discrete)))	EPO; JPO; DERWENT	2002/12/30 05:01

8	16	((((database$1 OR register$1 OR registr$3 OR administrator$1 OR agent$1 OR vendor$ OR server$1 OR station$1) SAME ((person$4 OR user$2 OR subscriber$2 OR customer$2 OR individual$2 OR party$1) NEAR4 (information OR data OR attribute$1 OR detail$1 OR characteristic$1)) SAME (((secur$4 OR access$4 OR authoriz$6 OR authoris$6) NEAR4 (level$1 OR categor$3 OR option$1)) OR privilege$1))) AND ((person$4 OR user$2 OR subscriber$2 OR customer$2 OR individual$2 OR party$1) NEAR4 (information OR data OR attribute$1 OR detail$1 OR characteristic$1)) WITH (transmi$6 OR send$4 OR forward$4 OR transfer$6 OR receiv$4 OR download$4 OR retriev$4)) AND (((secur$4 OR access$4 OR authoriz$6 OR authoris$6 OR privilege$1) NEAR4 (level$1 OR categor$3 OR option$1 OR zon$3 OR layer$3 OR grain$1 OR granular$4 OR discrete)))) AND (request$4 SAME (((person$4 OR user$2 OR subscriber$2 OR customer$2 OR individual$2 OR party$1) NEAR4 (information OR data OR attribute$1 OR detail$1 OR characteristic$1)) WITH (transmi$6 OR send$4 OR forward$4 OR transfer$6 OR receiv$4 OR download$4 OR retriev$4)))	EPO; JPO; DERWENT	2002/12/30 05:02

9	12	(((((database$1 OR register$1 OR registr$3 OR administrator$1 OR agent$1 OR vendor$ OR server$1 OR station$1) SAME ((person$4 OR user$2 OR subscriber$2 OR customer$2 OR individual$2 OR party$1) NEAR4 (information OR data OR attribute$1 OR detail$1 OR characteristic$1)) SAME (((secur$4 OR access$4 OR authoriz$6 OR authoris$6) NEAR4 (level$1 OR categor$3 OR option$1)) OR privilege$1))) AND ((person$4 OR user$2 OR subscriber$2 OR customer$2 OR individual$2 OR party$1) NEAR4 (information OR data OR attribute$1 OR detail$1 OR characteristic$1)) WITH (transmi$6 OR send$4 OR forward$4 OR transfer$6 OR receiv$4 OR download$4 OR retriev$4)) AND (((secur$4 OR access$4 OR authoriz$6 OR authoris$6 OR privilege$1) NEAR4 (level$1 OR categor$3 OR option$1 OR zon$3 OR layer$3 OR grain$1 OR granular$4 OR discrete)))) AND (request$4 SAME (((person$4 OR user$2 OR subscriber$2 OR customer$2 OR individual$2 OR party$1) NEAR4 (information OR data OR attribute$1 OR detail$1 OR characteristic$1)) WITH (transmi$6 OR send$4 OR forward$4 OR transfer$6 OR receiv$4 OR download$4 OR retriev$4)))) NOT us.pc.	EPO; JPO; DERWENT	2002/12/30 05:02

10	7	((((((database$1 OR register$1 OR registr$3 OR administrator$1 OR agent$1 OR vendor$ OR server$1 OR station$1) SAME ((person$4 OR user$2 OR subscriber$2 OR customer$2 OR individual$2 OR party$1) NEAR4 (information OR data OR attribute$1 OR detail$1 OR characteristic$1)) SAME (((secur$4 OR access$4 OR authoriz$6 OR authoris$6) NEAR4 (level$1 OR categor$3 OR option$1)) OR privilege$1))) AND ((person$4 OR user$2 OR subscriber$2 OR customer$2 OR individual$2 OR party$1) NEAR4 (information OR data OR attribute$1 OR detail$1 OR characteristic$1)) WITH (transmi$6 OR send$4 OR forward$4 OR transfer$6 OR receiv$4 OR download$4 OR retriev$4)) AND (((secur$4 OR access$4 OR authoriz$6 OR authoris$6 OR privilege$1) NEAR4 (level$1 OR categor$3 OR option$1 OR zon$3 OR layer$3 OR grain$1 OR granular$4 OR discrete)))) AND (request$4 SAME (((person$4 OR user$2 OR subscriber$2 OR customer$2 OR individual$2 OR party$1) NEAR4 (information OR data OR attribute$1 OR detail$1 OR characteristic$1)) WITH (transmi$6 OR send$4 OR forward$4 OR transfer$6 OR receiv$4 OR download$4 OR retriev$4)))) NOT us.pc.) AND (@pd<20000107)	EPO; JPO; DERWENT	2002/12/30 05:03

PAT-NO: EP000844767A1

DOCUMENT-IDENTIFIER: EP 844767 A1

TITLE: User controlled browser

PUBN-DATE: May 27, 1998

INVENTOR-INFORMATION:

NAME	COUNTRY
ROWLAND, BRUCE R	US
FRIEDMAN, LEE G	US

ASSIGNEE-INFORMATION:

NAME	COUNTRY
NCR INT INC	US

APPL-NO: EP97306102

APPL-DATE: August 11, 1997

PRIORITY-DATA: US75242196A (November 19, 1996)

INT-CL (IPC): H04L029/06

EUR-CL (EPC): H04L029/06 ; G06F001/00

ABSTRACT:

CHG DATE=19990617 STATUS=O> A mechanism provides a **user-controlled information** disclosure process. A **user information database** (206,208), a BrowserID Client applet (406), and a BrowserID Website **database** (408) are configured at a user terminal (102). The **user information database** contains a plurality of **information records about a user's identification information and access levels** for the respective information records. The BrowserID Website **database** contains the names of web sites and **access levels** for the respective web sites.

In response to a **request for user information** from a web site, the BrowserID
Client applet checks the existing **access level** in the BrowserID Website
database for the web site (or negotiates a new **level), and if appropriate,**
retrieves the access key granted by the web site to gain access to a controlled
portion of a website. <IMAGE>

PAT-NO: EP000844767A1

DOCUMENT-IDENTIFIER: EP 844767 A1

TITLE: User controlled browser

PUBN-DATE: May 27, 1998

INVENTOR-INFORMATION:

NAME	COUNTRY
ROWLAND, BRUCE R	US
FRIEDMAN, LEE G	US

ASSIGNEE-INFORMATION:

NAME	COUNTRY
NCR INT INC	US

APPL-NO: EP97306102

APPL-DATE: August 11, 1997

PRIORITY-DATA: US75242196A (November 19, 1996)

INT-CL (IPC): H04L029/06

EUR-CL (EPC): H04L029/06 ; G06F001/00

ABSTRACT:

CHG DATE=19990617 STATUS=O> A mechanism provides a **user-controlled information** disclosure process. A **user information database** (206,208), a BrowserID Client applet (406), and a BrowserID Website **database** (408) are configured at a user terminal (102). The **user information database** contains a plurality of **information records about a user's identification information and access levels** for the respective information records. The BrowserID Website **database** contains the names of web sites and **access levels** for the respective web sites.

In response to a **request for user information** from a web site, the BrowserID
Client applet checks the existing **access level** in the BrowserID Website
database for the web site (or negotiates a new **level), and if appropriate,**
retrieves the access key granted by the web site to gain access to a controlled
portion of a website. <IMAGE>

L Number	Hits	Search Text	DB	Time stamp
1	772	(((database$1 OR register$1 OR registr$3 OR administrator$1 OR agent$1 OR vendor$ OR server$1 OR station$1) SAME ((person$4 OR user$2 OR subscriber$2 OR customer$2 OR individual$2 OR party$1) NEAR4 (information OR data OR attribute$1 OR detail$1 OR characteristic$1)) SAME (((secur$4 OR access$4 OR authoriz$6 OR authoris$6) NEAR4 (level$1 OR categor$3 OR option$1)) OR privilege$1))) AND ((person$4 OR user$2 OR subscriber$2 OR customer$2 OR individual$2 OR party$1) NEAR4 (information OR data OR attribute$1 OR detail$1 OR characteristic$1)) WITH (transmi$6 OR send$4 OR forward$4 OR transfer$6 OR receiv$4 OR download$4 OR retriev$4)	USPAT	2002/12/30 03:44
2	665	((((database$1 OR register$1 OR registr$3 OR administrator$1 OR agent$1 OR vendor$ OR server$1 OR station$1) SAME ((person$4 OR user$2 OR subscriber$2 OR customer$2 OR individual$2 OR party$1) NEAR4 (information OR data OR attribute$1 OR detail$1 OR characteristic$1)) SAME (((secur$4 OR access$4 OR authoriz$6 OR authoris$6) NEAR4 (level$1 OR categor$3 OR option$1)) OR privilege$1))) AND ((person$4 OR user$2 OR subscriber$2 OR customer$2 OR individual$2 OR party$1) NEAR4 (information OR data OR attribute$1 OR detail$1 OR characteristic$1)) WITH (transmi$6 OR send$4 OR forward$4 OR transfer$6 OR receiv$4 OR download$4 OR retriev$4)) AND (((secur$4 OR access$4 OR authoriz$6 OR authoris$6 OR privilege$1) NEAR4 (level$1 OR categor$3 OR option$1 OR zon$3 OR layer$3 OR grain$1 OR granular$4 OR discrete)))	USPAT	2002/12/30 03:45

4	46	((((((database$1 OR register$1 OR registr$3 OR administrator$1 OR agent$1 OR vendor$ OR server$1 OR station$1) SAME ((person$4 OR user$2 OR subscriber$2 OR customer$2 OR individual$2 OR party$1) NEAR4 (information OR data OR attribute$1 OR detail$1 OR characteristic$1)) SAME (((secur$4 OR access$4 OR authoriz$6 OR authoris$6) NEAR4 (level$1 OR categor$3 OR option$1)) OR privilege$1))) AND ((person$4 OR user$2 OR subscriber$2 OR customer$2 OR individual$2 OR party$1) NEAR4 (information OR data OR attribute$1 OR detail$1 OR characteristic$1)) WITH (transmi$6 OR send$4 OR forward$4 OR transfer$6 OR receiv$4 OR download$4 OR retriev$4)) AND (((secur$4 OR access$4 OR authoriz$6 OR authoris$6 OR privilege$1) NEAR4 (level$1 OR categor$3 OR option$1 OR zon$3 OR layer$3 OR grain$1 OR granular$4 OR discrete)))) AND (request$4 SAME (((person$4 OR user$2 OR subscriber$2 OR customer$2 OR individual$2 OR party$1) NEAR4 (information OR data OR attribute$1 OR detail$1 OR characteristic$1)) WITH (transmi$6 OR send$4 OR forward$4 OR transfer$6 OR receiv$4 OR download$4 OR retriev$4)))) AND ((((secur$4 OR access$4 OR authoriz$6 OR authoris$6 OR privilege$1) NEAR4 (level$1 OR categor$3 OR option$1 OR zon$3 OR layer$3 OR grain$1 OR granular$4 OR discrete))) SAME ((person$4 OR user$2 OR subscriber$2 OR customer$2 OR individual$2 OR party$1) NEAR4 (information OR data OR attribute$1 OR detail$1 OR characteristic$1) NEAR4 (part$1 OR portion$1 OR piece$1 OR certain OR particular)))	USPAT	2002/12/30 04:47

3	344	((((database$1 OR register$1 OR registr$3 OR administrator$1 OR agent$1 OR vendor$ OR server$1 OR station$1) SAME ((person$4 OR user$2 OR subscriber$2 OR customer$2 OR individual$2 OR party$1) NEAR4 (information OR data OR attribute$1 OR detail$1 OR characteristic$1)) SAME (((secur$4 OR access$4 OR authoriz$6 OR authoris$6) NEAR4 (level$1 OR categor$3 OR option$1)) OR privilege$1))) AND ((person$4 OR user$2 OR subscriber$2 OR customer$2 OR individual$2 OR party$1) NEAR4 (information OR data OR attribute$1 OR detail$1 OR characteristic$1)) WITH (transmi$6 OR send$4 OR forward$4 OR transfer$6 OR receiv$4 OR download$4 OR retriev$4)) AND (((secur$4 OR access$4 OR authoriz$6 OR authoris$6 OR privilege$1) NEAR4 (level$1 OR categor$3 OR option$1 OR zon$3 OR layer$3 OR grain$1 OR granular$4 OR discrete)))) AND (request$4 SAME (((person$4 OR user$2 OR subscriber$2 OR customer$2 OR individual$2 OR party$1) NEAR4 (information OR data OR attribute$1 OR detail$1 OR characteristic$1)) WITH (transmi$6 OR send$4 OR forward$4 OR transfer$6 OR receiv$4 OR download$4 OR retriev$4)))	USPAT	2002/12/30 03:54

5	20	((((((database$1 OR register$1 OR registr$3 OR administrator$1 OR agent$1 OR vendor$ OR server$1 OR station$1) SAME ((person$4 OR user$2 OR subscriber$2 OR customer$2 OR individual$2 OR party$1) NEAR4 (information OR data OR attribute$1 OR detail$1 OR characteristic$1)) SAME (((secur$4 OR access$4 OR authoriz$6 OR authoris$6) NEAR4 (level$1 OR categor$3 OR option$1)) OR privilege$1))) AND ((person$4 OR user$2 OR subscriber$2 OR customer$2 OR individual$2 OR party$1) NEAR4 (information OR data OR attribute$1 OR detail$1 OR characteristic$1)) WITH (transmi$6 OR send$4 OR forward$4 OR transfer$6 OR receiv$4 OR download$4 OR retriev$4)) AND (((secur$4 OR access$4 OR authoriz$6 OR authoris$6 OR privilege$1) NEAR4 (level$1 OR categor$3 OR option$1 OR zon$3 OR layer$3 OR grain$1 OR granular$4 OR discrete)))) AND (request$4 SAME (((person$4 OR user$2 OR subscriber$2 OR customer$2 OR individual$2 OR party$1) NEAR4 (information OR data OR attribute$1 OR detail$1 OR characteristic$1)) WITH (transmi$6 OR send$4 OR forward$4 OR transfer$6 OR receiv$4 OR download$4 OR retriev$4)))) AND ((((secur$4 OR access$4 OR authoriz$6 OR authoris$6 OR privilege$1) NEAR4 (level$1 OR categor$3 OR option$1 OR zon$3 OR layer$3 OR grain$1 OR granular$4 OR discrete))) SAME ((person$4 OR user$2 OR subscriber$2 OR customer$2 OR individual$2 OR party$1) NEAR4 (information OR data OR attribute$1 OR detail$1 OR characteristic$1) NEAR4 (part$1 OR portion$1 OR piece$1 OR certain OR particular)))) AND ((((secur$4 OR access$4 OR authoriz$6 OR authoris$6) NEAR4 (key$1 OR code$1 OR number$1 OR value$1 OR sequence$1 OR challenge$1)) OR password$1 OR PIN$1 OR identif$6) SAME (((person$4 OR user$2 OR subscriber$2 OR customer$2 OR individual$2 OR party$1) NEAR4 (information OR data OR attribute$1 OR detail$1 OR characteristic$1)) WITH (transmi$6 OR send$4 OR forward$4 OR transfer$6 OR receiv$4 OR download$4 OR retriev$4))	USPAT	2002/12/30 04:50

US-PAT-NO: 6148342

DOCUMENT-IDENTIFIER: US 6148342 A

TITLE: Secure database management system for confidential records using
separately encrypted identifier and access request

---------- KWIC ---------

This invention relates to protecting confidential information. In particular,
the invention prevents insiders with high **levels of computer access** from
accessing sensitive data.

Computer systems have long been used for processing sensitive information.
Such systems typically include a **database** and a processor which manipulates
large amounts of highly **personal and confidential data**. In order to protect
outsiders from accessing the confidential data, fire walls and encryption
systems are often used to prevent unauthorized access to the data. Examples of
traditional systems and methods used to prevent unauthorized access to
sensitive **data include such mechanisms as user** authentication, **access location restriction, and user level access** controls. Although such systems are useful
for preventing "outsiders" from accessing confidential data, these systems are
typically unable to protect the data from "insiders" who have been granted high
enough system access **privileges** to bypass the security controls. In
particular, it is very difficult to deny a system **administrator** access to
sensitive or confidential data.

System administrators who have a high **level of access** can

typically access most
data on the computer system. As data on the computer becomes increasingly
sensitive and valuable, the system administrator or other "trusted insider"
increasingly has incentives to defeat the protection mechanisms of the system
and sell the confidential data. Thus, a system which is capable of storing
confidential data in a form that is inaccessible to high-level computer
administrators while still granting access to sensitive data to appropriate
parties is needed.

A method for retrieving sensitive stored data is described. A receiving
terminal receives a request for data from a user and encrypts an identifier
with a first code and a data access request with a second code. The identifier
and data access request are transmitted to a first database which decodes the
identifier and determines whether the user has authorization to request the
desired information. The first database then retrieves an associated access
level and internal identifier. The first database forwards the still encrypted
data access request with the associated access level and internal identifier to
a second database.

The second database retrieves the information requested in the data access
request and in one embodiment, if the user has an appropriate access level,
transmits the requested information to the receiving terminal.

In one embodiment of the invention, the secure system is implemented using a
large network of subnetworked computers. For example, the Internet represents
a large network which couples together subnetworks such as a local area network

or ethernet coupled computers. For optimal security, each of the subnetworks described will be under the control of a different administrator. Each administrator will not have control over computers outside of the respective subnetwork. By partitioning sensitive data and distributing storage and **retrieval** of sensitive data over different subnetworks of computers, the **data will be protected from improper access by an individual** administrator of a subnetwork.

FIG. 1 illustrates a secure data management system 100 used to implement one embodiment of the invention. A user inputs data into a source terminal 104. A typical user may be a doctor or other personnel with an appropriate **level of access** to request the needed data. In one embodiment, source terminal 104 may be a computer, or other processing device, including a personal computer. In an alternate embodiment, source terminal 104 is merely a terminal coupled to a main frame computer or other processing device. The source terminal may be associated with a local computer network or "source subnetwork" 106. Source subnetwork 106 may be a plurality of computers connected by a local area network. Source terminal 104 identifies or collects information to identify the user, typically by obtaining passwords, handprints, fingerprints, retinal scans, or other appropriate identification mechanism. After verification of the user's identity, the user, for example, a doctor, a lawyer, drug enforcement personnel, government official or banker, who has a need to know the information, requests access to specific **information about a particular individual subject which is processed by the secure data** management system 100. The user can also be a computer program or system.

Source terminal 104 **receives information from the user and combines the information** into a data packet 116 for output to other sections of secure system 100. The data packet 116 is composed of two smaller data packets, an identifier 112 and a data access **request** 124. Identifier 112 includes subdata packets such as user I.D. 118 and subject I.D. 120. The first subdata packet, user I.D. 118, includes information on the user such as information needed to identify the doctor **requesting** data. Such information may include, but is not limited to the last name, first name, middle name, social security number, birth date, mother's maiden name, driver's license, medical license number, state bar number, drug enforcement agency number, invoice number, fingerprint number, or other information necessary or useful for identifying the user **requesting** the data. Second subdata packet, subject I.D. 120, includes information about the subject. The information in the second subdata package includes data needed to identify the individual or entity relating to the data access **request**. Such information may, for example, include the last name, first name, middle name, social security number, birth date, birthplace, mother's maiden name, driver's license, street address, e-mail, file number, patient identification number, inmate identification number, account number, or name of company.

Identifier **database** 128 uses the information contained in identifier 112 to generate (1) an **access level indicating the access** allowances of the **user requesting data,** and (2) an internal identifier identifying the **individual or entity (the subject) corresponding to the requested data**. Identifier 112

information serves as a search key to query a database, typically a table 132.
In one embodiment, the user requesting data, specified by user I.D. 118, is used to identify data for lookup in table 132 and determine the user's approved access level in relation to the individual identified in subject I.D. section 120. In particular, the subnetwork 130 determines the types of data access activities that the user is permitted to perform on the records relating to the subject identified by subject I.D. 120. For example, the subnetwork 130 may determine whether the user is a doctor currently treating the identified individual. When a doctor is identified as treating an identified individual, the doctor is associated with a corresponding access level to permit the doctor to review x-ray, lab results, or add a progress note to the patient's records.
The subnetwork 130 containing identifier database 128 associates an authorized user access level to the doctor. Identifier database 128 assigns a Subject Internal I.D., typically using a table such as table 133, to the individual identified in Subject I.D. Section 120 of identifier 112.

The identifier database 128 outputs a data packet 148 including (1) a subject data section 144, and (2) a data access request 124. In one embodiment, the subject data section 144 includes a user access level subsection 136 and an internal identifier stored in a subject internal identifier subsection 140.
Subject data section 144 may also include the address of the originating source terminal 104. Because the material contained in subject data section 144 is typically incomprehensible to an interloper, it is not required that the subject data section 144 be encrypted. In maximum security systems, subject material in subject data 144 is encrypted with a code such

that the subject material is only readable by data request database 152. In one embodiment of the invention, the identity of the user and the subject, the address of source terminal 104 and the time at which data was received and/or transmitted is stored in a log 156 in identifier database 128.

Data request database 152 and the associated subnetwork 154 receives data packet 148. When subject data 144 is encrypted, data request database 152 decrypts the subject data section 144 of data packet 148 and retrieves the subject internal I.D. 140 and the user access level 136. Data request database 152 also decrypts the data access request 124. Data access request 124 of data packet 148 is encrypted using a code readable only by data request database 152. In one embodiment of the invention, source terminal 104 encrypts data access request 124 with the public key of data request database 152 allowing data request database 152 to retrieve the data access request 124 using a corresponding private key.

Data request database 152 determines if the user access level is sufficient to perform the type of data access requested in data access request 124 upon the records corresponding to the subject internal identifier 140. When the user has an appropriate user access level and is thus entitled to perform the operation, the data request database 152 performs the requested operation upon records keyed to the internal identifier 140.

Within the identifier database, the identifier information is decrypted in block 220. Typically, decryption is done using the private key of the identifier database. In block 224, identifier database uses the decrypted

identifier **information to look-up the individual for whom data** is requested (subject), such as a patient in a hospital, and makes sure that such person or entity exists. The identifier **database** also verifies that the individual requesting the access has the authority to access the subject's information in block 224. For example, the subject may be a patient in a hospital and the **person requesting the data** may be a doctor. When used in a hospital, the identifier **database** may check a table to make sure that the patient and the doctor represent a doctor-patient pair in block 224. If the doctor and patient do not form a doctor-patient pair, access is not allowed in block 230 and the source terminal is notified that the information is not available in block 232. If the doctor and patient are a doctor-patient pair, then access is allowed in decision block 230 and the **database** retrieves the (1) appropriate **privilege level** corresponding to the doctor-patient pair and (2) the internal ID corresponding to the patient in block 236.

The identifier database encrypts the internal ID, the **privilege level,** and the source terminal address in block 240 for transmission to a data request database in a separately administered subnetwork. The actual patient name as well as the doctor name is stripped from the data, identified only by an internal ID. In one embodiment of the invention, identifier database encrypts the internal ID with the public key of the data request database. In block 244 of FIG. 2B, the data packet including the internal identifier, user **access level or privilege level,** along with the original encrypted data access request, is transmitted to the data request database in block 244. In one embodiment, an entry is added to a log to document the

transmission in block 244. The transmission may be through a dedicated line or virtual private network to ensure data security and integrity. In one embodiment, the entire packet is encrypted and signed.

In block 248, the data request database decrypts the information received from the identifier database. In block 252, the data request database retrieves the patient's medical records file corresponding to the internal identifier. In decision block 256, the data request database determines if access to the particular information in the file is allowed based on the **access privilege level** received. If access is not allowed, a notice is sent to the source terminal in block 260.

When the **privilege level authorizes** access to the specific information, the data request **database** performs the requested operation and encrypts the result set in a data packet for transmission to the source terminal. In one embodiment, the requested information is encrypted with the public key of the source terminal in block 264. The public key of the source terminal could have been received with the data access request. The encrypted data is then transmitted back to the source terminal in block 268. The source terminal decodes the **data and displays it to the authorized user**.

FIG. 3C illustrates a system including a single user 300 and multiple data **request** databases 350, 354. Multiple data **request** databases divide and thereby reduce the amount of information processed and controlled by each administrator of each data **request** database 350, 354. Partitioning the information improves security. In FIG. 3C, the user at the source terminal partitions and encrypts

data for each of the data request database units 350, 354. The identifier database 358 verifies the identity of user 300 and forwards the partitioned and encrypted data to the respective first data request database 350 and/or second data request database 354. In one embodiment of the invention, each data request database 350, 354 has its own corresponding public-private encryption key-pairs to secure of transmission between user 300 and each of the data request databases 350, 354. Each data request database 350, 354 responds to the request and transmits its response directly back to user 300 which recombines the responses.

In system 400 illustrated in FIG. 4, a user 404 transmits a data request with user and subject identifying information to a first identifier database 408 in a chain of identifier databases. Each identifier database 408, 412, 416 in the chain verifies a specific unit of user or subject identifying data. For example, first identifier database 408 may contain the name of the subject. When the first identifier database confirms the data, such as the name, the first identifier database 408 forwards the query to a second identifier database 412. Second identifier database 412 further verifies the identity of the subject by comparing a second unit of information such as a Social Security number of the subject to the received data. When the information is again verified, the second identifier database 412 communicates the request to a third identifier database 416 which may compare a third unit of data such as a fingerprint to verify the identity of the subject of the query.

Each identifier database keeps user 404 informed of the query progress through

the various identifier databases using return data paths 420, 424, 428.
Records belonging to the same subject (or user) are linked between identifier
databases using an internal identification. For example, each identifier
database in an identifier database pair such as identifier database pairs 412,
416 share a common internal identification. User 404 encrypts data for each
identifier database 408, 412, 416 with a public key of that identifier
database. When all three identifier databases 408, 412, 416 verify that the
subject or **user 404 is satisfactorily identified, data request** database 432
receives the data access **request and transmits** the response to the **user 404**
along data path 436.

8. The apparatus of claim 7 wherein the processor verifies that a user issuing
the data **access request has an appropriate access level**.

9. The apparatus of claim 8 wherein the processor transmits the data access
request to the second apparatus after a verification that the source has the
appropriate **access level**.